IN THE CLAIMS

1. (Previously presented) Apparatus for secure management of data in a computer controlled storage system comprising:

a trusted data management server (tdm server), responsive to a user or user program application, capable of storing data in and retrieving data from a storage system that comprises:

security structure generator means to generate the following security management structures:

a unique identifier for said data;

access control information for said data;

a data signature for authenticating said data from said data and said unique identifier; and

an access control information signature for authenticating said access control information from said access control information and said unique identifier.

2. (Previously presented) The apparatus of claim 1 further comprising:

encryption means for encrypting:

said data; and

said access control information, when required by said tdm server.

3. (Original) The apparatus of claim 2 wherein said encryption means is adapted to encrypt said data and said access control information.

4. (Previously presented) The apparatus of claim 2 further comprising:

storage control means for causing said storage system to store said security management structures and said data.

5. (Original) The apparatus of claim 4 wherein said data is stored in encrypted form.

6. (Previously presented) The apparatus of claim 5 further comprising:

access control means for accessing said data stored in said storage system with said unique identifier

7. (Previously presented) The apparatus of claim 6 wherein said access control means comprises:

means responsive to a request from ~~an~~ a user for accessing secured data from said storage system, adapted to:

retrieve a unique identifier for said data from said user or storage system;

retrieve from said storage system said security management structures corresponding to said data; and

carry out the following determination steps:

determine if said access control information and unique identifier correspond with said access control information signature;

determine if said data and its unique identifier correspond with said data signature;

determine if said unique identifier of said access control information corresponds with said unique identifier of said secured data; and

determine whether said access control information permits said user to access said secured data; and then grant access to said user to said data if each of said determination steps is satisfied, and otherwise refuse access.

8. (Original) The apparatus of claim 7 wherein said access control means further includes means to notify said user if access is refused.

9. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Previously presented) A method for secure management of data in a computer controlled storage system comprising:

in a trusted data management server (tdm server), responsive to a user or user program application, for storing data in and retrieving data from a storage system generating the following security management structures:

a unique identifier for said data;

access control information for said data;

a data signature for authenticating said data from said data and said unique identifier; and

an access control information signature for authenticating said access control information from said access control information and said unique identifier.

13. (Original) The method of claim 12 further comprising:
encrypting said data, or said access control information.

14. (Original) The method of claim 13 comprising encrypting said data and said access control information.

15. (Previously presented) The method of claim 13 further comprising:
causing said storage system to store said security management structures and said data.

16. (Original) The method of claim 15 wherein said data is stored encrypted

17. (Original) The method of claim 16 further comprising:
accessing said data stored in said storage with said unique identifier

18. (Previously presented) The method of claim 16 responsive to a request from a user for accessing data from said storage system, retrieving a unique identifier for said data from said user or database storage;

retrieve from said storage system said security management structures corresponding to said secured data; and

carrying out the following determination steps:

determine if said access control information and its unique identifier correspond with said access control information signature;

determine if said secured data and its unique identifier correspond with said data signature;

determine if said unique identifier of said access control information corresponds with said secured data; and

determine whether said access control information permits said user to access said secured data; and then granting access to said user to said data if each of said determination steps is satisfied, and otherwise refusing access.

19. (Original) The method of claim 18 including notifying said user if access is refused.

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system of the method of claim 13.

24. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system for causing the computer system to effect the apparatus of claim 1.

25. (Canceled)

26. (Canceled)

27. (Previously presented) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing secure management of data in a computer controlled storage system, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 12.

28. (Canceled)

29. (Canceled)

30. (Previously presented) A method for storing a document in a secure storage system comprising the steps of:

submitting the document for secure storage;

generating a random number at a trusted document management server;

requesting a database management system to reserve the generated random number as a document key;

computing a digital document signature at the trusted document management server, wherein the document signature is capable of authenticating document content and the document key;

creating an initial access control list (ACL) at the trusted document management server;

computing a digital ACL signature at the trusted document management sever, wherein the ACL signature is capable of authenticating ACL content and the document key; and

instructing the database management system to store the document, the document signature, the ACL and the ACL signature.

31. (Canceled)